Abstract of Cited Ref. 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **04-306760**
(43)Date of publication of application : **29.10.1992**

(51)Int.Cl. G06F 15/00
G06F 15/30
G06F 15/30
G06K 17/00
G07F 7/12
G09C 1/00

(21)Application number : **03-098017**
(22)Date of filing : **03.04.1991**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**
(72)Inventor : **MORITA HIKARI**
KURIHARA SADAMI

(54) RECOGNITION METHOD FOR POSSESSOR OF CARDS

(57)Abstract:
PURPOSE: To securely recognize the right possessor of cards without increasing the burden on a user in an information processing service system using the cards.
CONSTITUTION: A processing/storage means is embedded in the belongings 1 (watch, ring and the like) of the possessor of the cards 2. The belongings 1 and the cards 2 previously share the same initial values of ciphered key data and output feedback data. At the time of using the cards 2, the belongings 1 cipher and update the output feedback data with ciphered key data and transmit the updated data to the cards 2. The cards 2 cipher and update the output feedback data with ciphered key data and compare the updated data with the updated data from the cards 1. When they coincide, the cards concerned are set to a usable state. Here, the access of an information processor 3 by the cards 2 becomes possible.

Cited Ref. 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平4－306760

(43)公開日　平成４年(1992)10月29日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ｂ	7323－5L		
		Ｆ	7323－5L		
	15/30	３４０	6798－5L		
		３５０	6798－5L		
			8818－3E	Ｇ０７Ｆ　7／08　Ｂ	

審査請求　未請求　請求項の数６(全 10 頁)　最終頁に続く

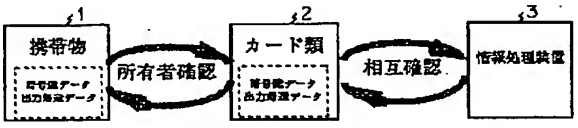
(21)出願番号　特願平3－98017

(22)出願日　平成３年(1991)４月３日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　森田　光
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(72)発明者　栗原　定見
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　鈴木　誠

(54)【発明の名称】　カード類の所有者確認方法

(57)【要約】
【目的】　カード類を利用する情報処理サービスシステムにおいて、使用者の負担を増加させることなく、確実にカード類の正当所有者の確認を行う。
【構成】　カード類２の所有者の携帯物１（時計、指輪等）に処理／記憶手段を埋め込み、携帯物１とカード類２とに、予め同一の暗号鍵データと出力帰還データの初期値を共有させる。カード類２を利用する際、携帯物１は、その出力帰還データを暗号鍵データで暗号化して更新すると共に、該更新データをカード類２に送る。カード類２でも、その出力帰還データを暗号鍵データで暗号化して更新し、該更新データとカード類１からの更新データを比較し、一致したら当該カード類を利用可状態とする。ここで初めて、カード類２による情報処理装置３のアクセスが可能となる。



1

【特許請求の範囲】

【請求項１】　利用可と利用不可の状態をとり、利用可の場合に情報処理装置に対して処理を依頼でき、処理終了で利用不可となるカード類の所有者を確認する方法であって、前記カード類の所有者が携帯する携帯物に、あらかじめ定めた暗号鍵データを格納する手段と、あらかじめ定めた初期値をとり、その後更新される出力帰還データを格納する手段と、前記暗号鍵データにより前記出力帰還データを暗号化して更新する手段と、前記更新された出力帰還データを前記カード類に送信する手段を設け、前記カード類には、前記携帯物が送信した出力帰還データを受信する手段と、あらかじめ定めた暗号鍵データを格納する手段と、あらかじめ定めた初期値をとり、その後更新される出力帰還データを格納する手段と、前記暗号鍵データにより前記出力帰還データを暗号化して更新する手段と、前記更新された出力帰還データと前記携帯物から受信した出力帰還データとを比較して、当該カード類の利用可または利用不可を決定する手段とを設け、前記携帯物とカード類の暗号鍵データ、出力帰還データの初期値を一致させ、所有者の処理要求の度に、前記携帯物の出力帰還データと前記カード類の出力帰還データを更新せしめて同期をとることを特徴とするカード類の所有者確認方法。

【請求項２】　前記携帯物とカード類が同時に発行されない場合のために、前記カード類に１回だけ暗号鍵データと出力帰還データの初期値とを設定する手段を設けたことを特徴とする請求項１記載のカード類の所有者確認方法。

【請求項３】　前記カード類に比べて前記携帯物の出力帰還データが余分に更新される場合のために、前記カード類の出力帰還データを更新しつつ前記携帯物から受信した出力帰還データと複数回比較することを特徴とする請求項１記載のカード類の所有者確認方法。

【請求項４】　前記カード類が前記携帯物に比べて出力帰還データが余分に更新されるのを防ぐために、カード類に暗号化機能とその逆の復号機能を合せ持つ手段を設け、該カード類で利用不可の判定が下った時、該カード類の出力帰還データを当該確認開始時の元の出力帰還データへ戻すことを特徴とする請求項３記載のカード類の所有者確認方法。

【請求項５】　前記カード類が前記携帯物に比べて出力帰還データが余分に更新されるのを防ぐために、カード類に当該確認開始時の出力帰還データを保持する手段を設け、該カード類で利用不可の判定が下った時、該カード類の出力帰還データを当該確認開始時の元の出力帰還データへ戻すことを特徴とする請求項３記載のカード類の所有者確認方法。

【請求項６】　前記カード類と前記携帯物との確認処理と、利用可となってからのカード類と情報処理装置との相互処理に一定時間の間隔を許容するため、前記カード類に、該カード類を一定時間だけ利用可状態とし、該一定時間内に情報処理装置との相互処理が開始されないと自動的に利用不可状態にする手段を設けたことを特徴とする請求項１記載のカード類の所有者確認方法。

2

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、カード類を利用する情報処理サービスシステムなどにおいて、特に、利用可と利用不可の状態をとり、利用可の場合に情報処理装置に対して処理を依頼でき、処理終了で利用不可となるカード類を使用する場合の所有者確認方法に関する。

【０００２】

【従来の技術】従来、情報処理サービスシステムにおける個人確認の代表例としては、情報通信サービス分野でのコンピュータ端末からセンターへアクセスする時のパスワードや、キャッシュカード利用時に於ける暗証番号による確認などが知られている。しかし、コンピュータ利用のパーソナル化の進展に伴い、人間の忘却性、複数利用時の煩雑性、他人によるパスワード推測可能性などが問題になってきている。

【０００３】これらの要求条件を満たす個人確認技術に必須な構成要素としては、ＩＣカードを代表とするカード類が有効である。ここで、カード類とは、キャッシュカード、クレジットカード、プリペイドカードなど現在利用されている磁気タイプのカードや、データ入出力を抑止するインテリジェント機能を付加できるＬＳＩを組み込んだＩＣカードなどが挙げられる。

【０００４】限界ある個人の記憶情報に比べて、ＩＣカードに埋め込める認証子のデータ量は膨大であるため、最近の暗号・認証研究の成果であるＲＳＡ法、ＦＳ法など（例えば、辻井、笠原編著；“暗号と情報セキュリティ”、昭晃堂、１９９０．参照）によれば、高い確度で確認相手（対象装置）に対してカード類の識別を行うことが可能に成ってきている。

【０００５】

【発明が解決しようとする課題】ところで、情報処理装置等の対象装置に対してカード類を確認する機能が発達しても、真の所有者だけが利用できるようにならなければ安全ではない。従来のカード類の所有者確認方法は、図１４に示すように、記憶情報（暗証番号等）、所有物（クレジットカード、免許証等）、身体的特徴（指紋、筆跡等）に分類され、記憶情報や所有物が多用されている。このうち、記憶情報は人間の記憶のあいまいさに起因する問題がある。又、身体的特徴も、指紋等身体的特徴を対象とするパターン認識の研究は盛んであるが、操作性、コスト、確実性の観点から現状では解決すべき課題が多い。これに対し、個人の所有物による方法は実現的な解であるが、カード類の所有者を明らかにするための有効な手段が存在しないのが現状である。

【０００６】本発明の目的は、カード類では実現できな

い身体的特徴に匹敵する携帯性と、人間の記憶以上の確実性とを備え、複製しにくく紛失に気付き易い携帯物によるカード類の所有者確認方法を提供することにある。

【0007】

【課題を解決するための手段】上記目的を達成するために、本発明は、カード類の状態が利用可と利用不可の2種類あり、利用可の場合に該カード類により情報処理装置に対して処理を依頼でき、処理終了で利用不可となるとして、カード類の所有者が携帯する携帯物に、あらかじめ定めた暗号鍵データを格納する手段と、あらかじめ定めた初期値をとり、その後更新される出力帰還データを格納する手段と、前記暗号鍵データにより前記出力帰還データを暗号化して更新する手段と、前記更新された出力帰還データを前記カード類に送信する手段を設け、カード類には、前記携帯物が送信した出力帰還データを受信する手段と、あらかじめ定めた暗号鍵データを格納する手段と、あらかじめ定めた初期値をとり、その後更新される出力帰還データを格納する手段と、前記暗号鍵データにより前記出力帰還データを暗号化して更新する手段と、前記更新された出力帰還データと前記携帯物から受信した出力帰還データとを比較して、当該カード類の利用可または利用不可を決定する手段とを設け、前記携帯物とカード類の暗号鍵データ、出力帰還データの初期値を一致させ、所有者の処理要求の度に、前記携帯物の出力帰還データと前記カード類の出力帰還データを更新せしめて同期をとることを主たる特徴とするものである。

【0008】

【作用】本発明では、従来から用いられている個人識別のためのカード類に加えて、当該カード類の使用者であることを保証する手段として携帯物を導入し、携帯物とカード類で、あらかじめ同一の暗号鍵データと出力帰還データの初期値を共有し、該携帯物とカード類においてそれぞれ更新される出力帰還データを同期させることで、自動的に当該カード類の所有者確認を行う様にしたので、使用者の負担を増加させることなく、安全性の高い所有者確認を行うことが可能になる。

【0009】

【実施例】以下、本発明の実施例を図面にもとづいて詳細に説明する。図1は本発明の所有者確認方法を実施するシステムの基本構成の概念図を示したものである。図において、1はカード類所有者の携帯物、2は確認対象のカード類、3は目的の処理を実行する情報処理装置である。携帯物1としては、例えば、時計、ネクタイピン、指輪、またはブローチ等の装身具を用いて、これらの装身具内に処理／記憶手段を埋め込んで作る。また、カード類2としては、データ入出力等を任意に抑止するインテリジェント機能を付加できるＩＣカードを挙げることが出来る。これらの携帯物1とカード類2との結合は、電気的、光学的、または電磁的方法のいずれによっても良い。

【0010】正当な使用権を有する個人がカード類2により情報処理装置3を利用しようとする場合、当該利用者は、自分の携帯物1を用いてカード類2に自らが正当な所有者であることを確認させ、該確認されたカード類（利用可状態のカード類）2を情報処理装置3に接続等して目的の処理を依頼する。カード類2と情報処理装置3は相互に確認しあった後、情報処理装置3において目的の処理を実行し、それが完了すると、カード類2は利用不可状態となる。

【0011】図2に、所有者確認を行う場合の携帯物1とカード類2での処理概要を示す。同一所有者の携帯物1とカード類2には、あらかじめ同じ暗号鍵データと出力帰還データの初期値を記憶しておく。この携帯物1とカード類2の出力帰還データは、その後、所有者確認のたびに更新されるが、当該携帯物1とカード類2の処理が同期している限り、内容の一致性が保証される。

【0012】通常、カード類2は利用不可状態にある。該カード類2を用いて情報処理装置3に処理を依頼する場合、まず、利用者は携帯物1とカード類2を起動する。これは、利用者自身により携帯物1とカード類2の両方を起動してもよいし、図2に示すように、カード類2へは携帯物1から結合手段を介して確認要求を出すことでもよい。起動を受けた携帯物1は、記憶されている暗号鍵データにより出力帰還データを暗号化して前の出力帰還データを更新すると共に、該更新された出力帰還データをカード類2に送信する。カード類2でも、記憶されている暗号鍵データにより出力帰還データを暗号化して前の出力帰還データを更新するが、この更新された出力帰還データと携帯物1から送られた出力帰還データ（確認情報）とを照合し、一致したなら当該カード類2を利用可状態にする。このようにして、正当な所有者であることが確認されたなら、利用者は当該カード類2を情報処理装置3に接続して目的の処理を依頼する。そして、情報処理装置3での処理が完了すると、カード類2は自から利用不可状態に戻る。

【0013】以下に、本発明の所有者確認方法を実施するための種々のシステム構成を示す。

【0014】図3は本発明の第1の実施例の構成図である。携帯物1は、制御部１００、鍵レジスタ１０１、暗号化処理部１０２、送信部１０３、確認依頼受容部１０４、出力帰還データ（ＯＦＢ）レジスタ１１０から構成される。カード類2は、制御部２００、鍵レジスタ２０１、暗号化処理部２０２、受信部２０３、利用権情報管理部２０５、個人情報蓄積部２０６、情報処理装置対応処理部２０７、通信部２０８、ＯＦＢレジスタ２１０、照合部２１１から構成される。また、情報処理装置3は、制御部３００、個人情報蓄積部３０１、カード類対応処理部３０２、通信部３０３、目的処理部３０４から構成される。携帯物1とカード類2との接続手段１２

は、電気的、光学的、電磁的等のいずれによっても良い。

【００１５】所有者確認を行う前の前提条件として、携帯物１の鍵レジスタ１０１とカード類２の鍵レジスタ２０１には同一の暗号鍵を格納し、同様に、携帯物１のＯＦＢレジスタ１１０とカード類２のＯＦＢレジスタ２１０には同一の出力帰還データの初期値を格納しておく。各出力帰還データは、暗号鍵により暗号化処理された結果で更新されるため、ＯＦＢレジスタ１１０，２１０の出力帰還データは変化するが、該各出力帰還データを初期値で一致させれば、その後、同期して暗号化処理される限り、携帯物１とカード類２で一致が保証される。

【００１６】カード類２の所有者確認を行う場合、利用者は確認依頼受容部１０４を介して携帯物１へカード利用依頼を行い、カード類２へは携帯物１から接続手段１２を経由して確認要求を出力するか、利用者自らがカード類２へ確認要求を行うかして、結果的に携帯物１ならびにカード類２の制御部１００，２００が各処理部分を起動する。これにより、携帯物１では、暗号化処理部１０２がＯＦＢレジスタ１１０に格納されている出力帰還データを鍵レジスタ１０１に格納されている暗号鍵データで暗号化して更新し、該更新された出力帰還データを再びＯＦＢレジスタ１１０に格納する。同時に、該携帯物１の暗号化処理部１０２で更新された出力帰還データは、送信部１０３から送信され、接続手段１２を介してカード類２の受信部２０３で受信される。カード類２では、同様に暗号化処理部２０２がＯＦＢレジスタ２１０に格納されている出力帰還データを鍵レジスタ２０１に格納されている暗号鍵データを暗号化して更新し、該更新された出力帰還データを再びＯＦＢレジスタ２１０に格納する。さらに、該カード類２では、暗号化処理部２０２で更新された当該カード類２の出力帰還データと受信部２０３で受信された携帯物１の出力帰還データとを照合部２１１で比較し、両者が一致する場合、利用権情報管理部２０５のカード類利用状態を利用可状態へ切り替える。これでカード類２の利用が可能になる。

【００１７】カード類２が正当な所有者により使用されていることが確認されて、利用者がカード類２を情報処理装置３に接続すると、各制御部２００，３００の制御下で、以下の手順で処理が実行される。即ち、まず、カード類２と情報処理装置３では、個人情報蓄積部２０６，３０１に蓄積されている個人情報をもとに、情報処理装置対応処理部２０７とカード類対応処理部３０２で個人識別交信データを生成して、通信部２０８，３０３を介して交信し、相互に相手を確認しあう。そして、最終的に情報処理装置３のカード類対応処理部３０２がカード類２を正当と確認すると、次に、目的処理部３０４が当該カード類２の正当な所有者の求めている処理を実行し、それが完了すると、通信部３０３を介してカード類２に対して処理完了を通知する。カード類２の情報処理装置対応処理部２０７は、情報処理装置３より通信部２０８を介して処理完了を受け取ると、利用権情報管理部２０５のカード類利用状態を利用不可状態へ戻す。

【００１８】図４は、上述の処理フローをカード類２について表したものである。なお、図中で「携帯物出力情報不適合を表示」とあるのは、カード類２が情報処理装置３において目的処理を実行できなかったことで結果的に示すか、カード類２に接続される情報処理装置３経由で利用者に表示することなどを指す。

【００１９】図３の実施例は、ｘ＜＝ｅｋ（ｘ）（ｘを暗号鍵Ｋで暗号化して更新することを示す）で更新される出力帰還データは、例え第三者がある時の出力帰還データを知っても、暗号鍵Ｋを知らない限り、次の出力を推定することは困難であるという考えに基づいている。しかし、ｘの数列が短い周期の循環になる場合等、暗号化処理部１０２，２０２が実行する暗号化関数によっては、その関数に内在するアルゴリズム構造の欠陥を利用して、第三者が携帯物１からカード類２への送信データを推定する可能性は完全に排除できない。このような場合には、接続手段１２として電気接点による接続か、非接触の場合でも、指向性の高い電磁波（光波、赤外線等を含む）、超音波を用いる。この場合、携帯物１を所持する所有者が、携帯物の送信データを意識的に第三者に観測させない限り、観測が究めて困難となる。

【００２０】図５は本発明の第２の実施例の構成図で、図３の構成においてカード類２内に１タイム書き込み部２０４を付加したものである。

（１）安全上、カード類２と携帯物１とは異なる者が発行した方が一元的に秘密情報が管理される心配が無く好ましい。

（２）運用上等の要請で、カード類２と携帯物１との使用期間が異なる場合がある。

などの理由により、携帯物１とカード類２が、同時に発行されない場合がある。

【００２１】図５に於いては、その様な場合でも、カード類２に１タイム書き込み部２０４を備えることにより、携帯物１とカード類２との出力帰還データ同士の同期をとることが可能になる。即ち、カード類２に於て、携帯物１が保持している鍵レジスタ１０１に格納される暗号鍵とＯＦＢレジスタ１１０に格納される出力帰還データを、１タイム書き込み部２０４により最初の一回に限りそれぞれ鍵レジスタ２０１とＯＦＢレジスタ２１０に設定できるようにする。具体的には、書き込みが終了すると、ヒューズＲＯＭにデータが蓄積されるか、内部の論理処理を司る書き込みルーチンを消去させるなどで、外部からカード類２の鍵レジスタ２０１、ＯＦＢレジスタ２１０に対して書き込みができない状態として、１回だけの書き込みを可能とする。なお、携帯物１内のＯＦＢレジスタ１１０が可成更新された後に、新規のカード類２と対応付ける必要がある時、この１回だけの書

き込み時に限り、カード類２のＯＦＢレジスタ２１０の更新を多く繰り返すことで対応させる。

【００２２】図６は本発明の第３の実施例の構成図で、図３の構成においてカード類２内にカウンタ処理部２０９を付加したものである。

（１）複数のカード類２に携帯物１を対応付けたい。

（２）不用意な操作で携帯物１の出力帰還データが更新される可能性がある。

などの理由により、携帯物１とカード類２に格納される出力帰還データが同期しない場合がある。このような場合、一般に携帯物１の出力帰還データが余計に更新される。

【００２３】図６においては、カード類２にカウンタ処理部２０９を備えることにより、携帯物１の出力帰還データが余計に更新されていても、カード類２での出力帰還データの更新を所定回数繰り返すことで、正当な所有者を確認できる。

【００２４】図７に、カウンタ処理部２０９を付加した場合のカード類２における処理フローを示す。カード類２では、携帯物１が出力する出力帰還データと一致照合されるまで、該カード類内部で出力帰還データを更新する。適合しない携帯物を確認する場合、実用での携帯物における更新回数の上限をしきい値ＴＨとして設定し、そのしきい値までカード類の出力帰還データを更新しつつ一致照合をおこない、全て不一致なら適合しない携帯物と判定する。

【００２５】図８は本発明の第４の実施例の構成図で、図６の構成において、カード類２の暗号化処理部２０２を暗号化／復号処理部２０２’に置き換えたものである。

【００２６】図６の実施例では、対応付けられていない携帯物との照合によりカード類２の出力帰還データが更新されるが、この対策としては携帯物１の出力帰還データを更新すればよいことが考えられる。しかし、携帯物１の更新に、多大な操作または時間を要する場合など、携帯物更新が困難である場合、携帯物１よりカード類２の出力帰還データが余分に更新されることが、本所有者確認のシステムを構築する上での障害となることがある。このような場合、図８のように、カード類２の暗号化処理部を暗号化／復号処理部２０２’とすることにより、対応づけられていない携帯物と照合された時に生じるカード類２の出力帰還データの著しい更新を補償することができる。

【００２７】図９に、カウンタ処理部２０９に加え、暗号化処理部を暗号化／復号処理部２０２’に置き換えた場合のカード類２における処理フローを示す。カード類２に於いて、毎回行われる所有者確認では、携帯物１が出力する出力帰還データと一致照合されるまで、該カード類内部で出力帰還データを更新し、適合しない携帯物と判定された場合、カウンタの値が示す回数だけ、前回

正規の携帯物と確認した状態まで出力帰還データを、復号処理により遡る。

【００２８】図１０は本発明の第５の実施例の構成図で、図６の構成において、カード類２内にＯＦＢレジスタ２１０の他にサブＯＦＢレジスタ２１０’を追加したことである。本実施例の狙いは、図８の第４の実施例と同様に、カード類内の出力帰還データの更新が進み過ぎない様にする手段を提供することにある。図１１に、図１０の場合のカード類２における処理フローを示す。カード類２に於いて、毎回行われる所有者確認では、携帯物１が出力する出力帰還データと一致照合されるまで、該カード類内部で出力帰還データを更新し、適合しない携帯物が判定された場合、前回の利用可と判定された携帯物確認時の出力帰還データを格納していたサブＯＦＢレジスタ２１０’の値を読み出し、ＯＦＢレジスタ２１０に格納されていた値を元の出力帰還データへ戻す。なお、適合する携帯物と判定された場合は、サブＯＦＢレジスタ２１０’に、更新された出力帰還データが収容されたＯＦＢレジスタ２１０の値を書き込み、両者の値を一致させる。

【００２９】図１２は本発明の第６の実施例の構成図で、図３の構成においてカード類２内のタイマー２１２を付加したものである。

【００３０】携帯物１とカード類２間の所間者確認と、カード類２と情報処理装置３間の個人識別とは同時に行う必要がなく、両者の処理を行う場所が物理的に離れている方が好ましい場合がある。この為、図１２の実施例に於いては、所有者確認をしてから個人識別処理を行うまでの適当な期間を測定できるタイマー２１２をカード類２内に備えるようにしたものである。

【００３１】図１３に、タイマー２１２に関係するカード類２内の処理フローを示す。カード類２に於いて、カード類利用可状態へ切り替わった後で、タイマー２１２が０にリセットされ、最大許容経過時間以下の時間経過内に、目的処理の始まりである個人確認処理に移れば、正規の利用ができる。逆に最大許容経過時間より時間が経過すると、カード類は利用不可状態へ切り替わる。

【００３２】

【発明の効果】（1）請求項１の発明によれば、カード類では実現できない身体的特徴に匹敵する携帯性と、人間の記憶以上の確実性を備えた記憶手段として、時計、ネクタイピン、ブローチ等の装身具を携帯物を用いて、それに所定の機能を埋め込み、対応するカード類と同期をとることで、当該カード類の所有者確認を行うようにしたので、使用者の負担を増加させることなく、安全性の高い所有者確認を行うことができる。また、印鑑と同様の感覚で携帯物を利用できるため、指紋、顔形等の身体的特徴に比べ、人々に受け入れられ易い利点がある。さらに、装身具の形により多様な形態が可能であり応用範囲が広い利点もある。

9

【００３３】(2) 請求項２の発明によれば、携帯物とカード類が同時に発行されない場合においても、携帯物とカード類との出力帰還データ同士の同期をとることができる。

【００３４】(3) 請求項３の発明によれば、一つの携帯物を複数のカード類に対応付けした場合や、不用意な操作で携帯物の出力帰還データが更新された場合などにより、携帯物とカード類の出力帰還データが同期していない場合でも、支障なく所有者確認チェックを行うことができる。

【００３５】(4) 請求項４および５の発明によれば、請求項３において、対応付けられていない携帯物との照合によりカード類の出力帰還データが余分に更新される場合、自動的に確認チェック開始時の元の出力帰還データへ戻すことができる。

【００３６】(5) 請求項６の発明によれば、カード類と携帯物との確認処理と、利用可となってからのカード類と対象装置との相互処理に一定時間の間隔を許容するため、両者の処理を行う場所を物理的に離すことができる。

【図面の簡単な説明】

【図１】本発明が実施されるシステムの基本構成図である。

【図２】図１における携帯物とカード類の処理概要を示す図である。

10

【図３】本発明の第１の実施例の具体的構成図である。

【図４】図３におけるカード類の処理フロー図である。

【図５】本発明の第２の実施例の具体的構成図である。

【図６】本発明の第３の実施例の具体的構成図である。

【図７】図６におけるカード類の処理フロー図である。

【図８】本発明の第４の実施例の具体的構成図である。

【図９】図８におけるカード類の処理フロー図である。

【図１０】本発明の第５の実施例の具体的構成図である。

【図１１】図１０におけるカード類の処理フロー図である。

【図１２】本発明の第６の実施例の具体的構成図である。

【図１３】図１２におけるカード類内のタイマに関係する処理フロー図である。

【図１４】従来のカード類の所有者確認方法の一例を示した図である。

【符号の説明】

１　携帯物

２　カード類

３　情報処理装置

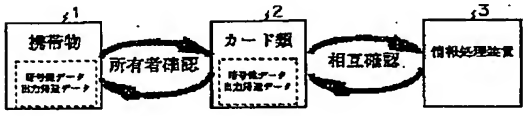
１０１，２０１　鍵レジスタ

１０２，２０２　暗号化処理部

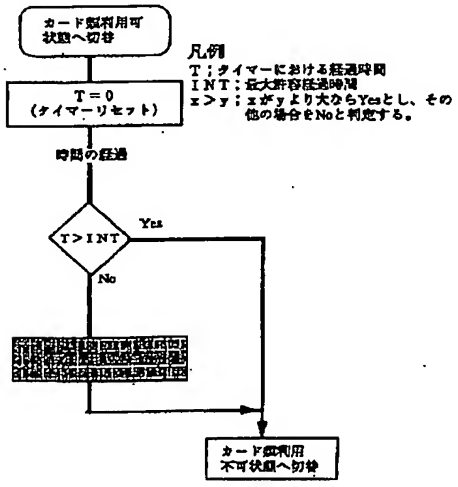
２１０　出力帰還データ（ＯＦＢ）レジスタ

１１１　照合部

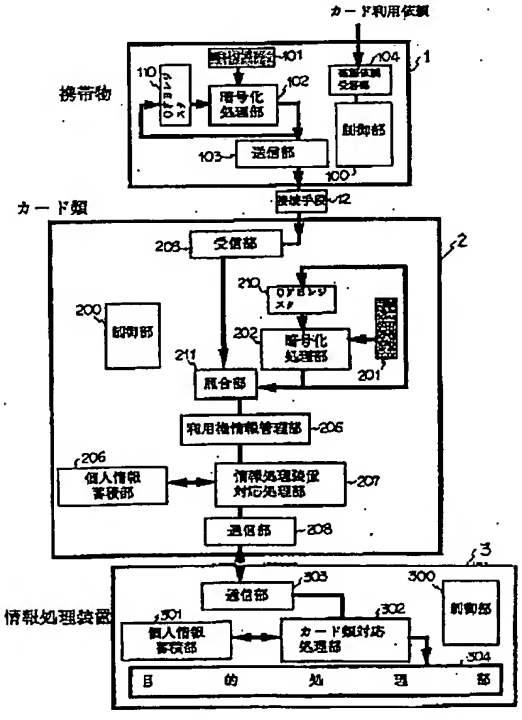
【図１】



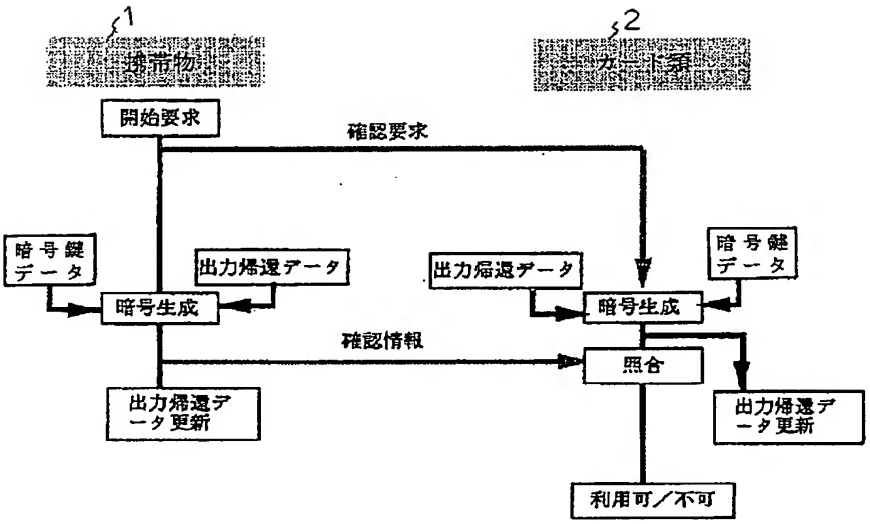
【図１３】



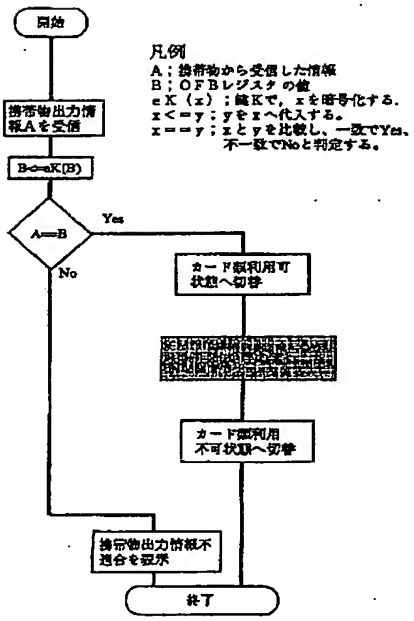
【図３】



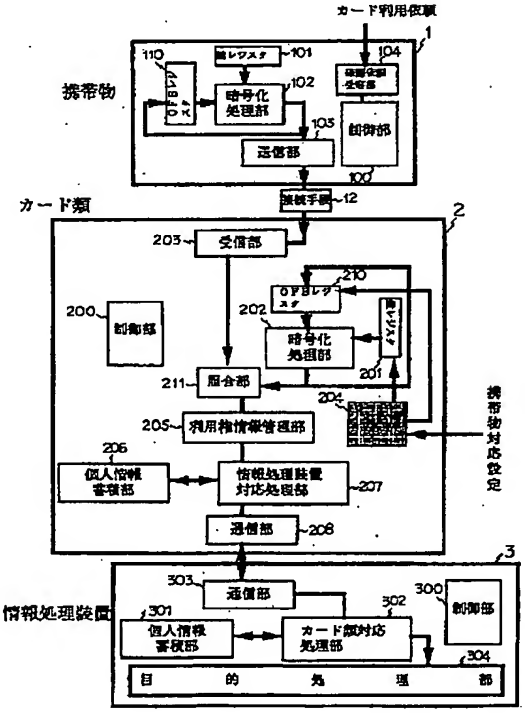
【図2】


1
携帯物
2
カード系
開始要求
確認要求
暗号鍵データ
出力帰還データ
出力帰還データ
暗号鍵データ
暗号生成
暗号生成
確認情報
照合
出力帰還データ更新
出力帰還データ更新
利用可／不可

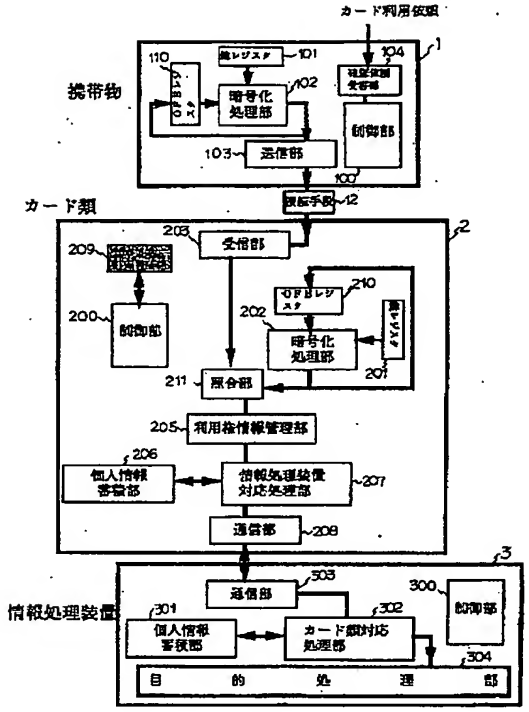
【図4】


開始
凡例
A；携帯物から受信した情報
B；OFBレジスタの値
eK（x）；鍵Kで，xを暗号化する．
x←y；yをxへ代入する。
x＝＝y；xとyを比較し、一致でYes、不一致でNoと判定する。
携帯物出力情報Aを受信
B←eK(B)
A==B
Yes
No
カード部利用可状態へ切替
カード部利用不可状態へ切替
携帯物出力情報不適合を表示
終了

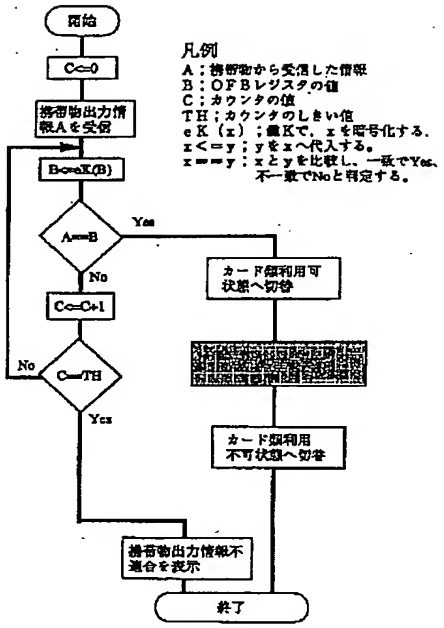
【図5】


カード利用依頼
1
携帯物
110
101
104
102
103
100
カード類
12
2
203
210
200
202
201
211
204
205
206
207
208
携帯物対応設定
3
情報処理装置
303
300
301
302
304
目的処理部

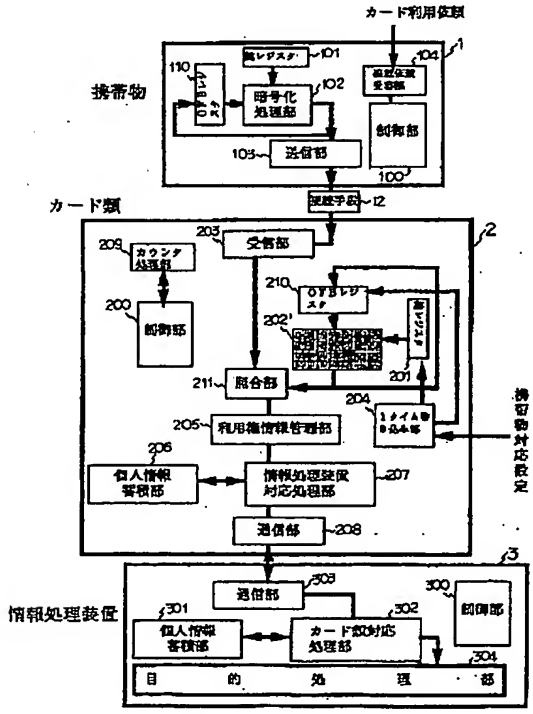
【図6】


カード利用依頼
携帯物
カード類
情報処理装置
暗号化処理部
送信部
制御部
受信部
照合部
利用者情報管理部
個人情報蓄積部
情報処理装置対応処理部
通信部
カード類対応処理部
目的処理部

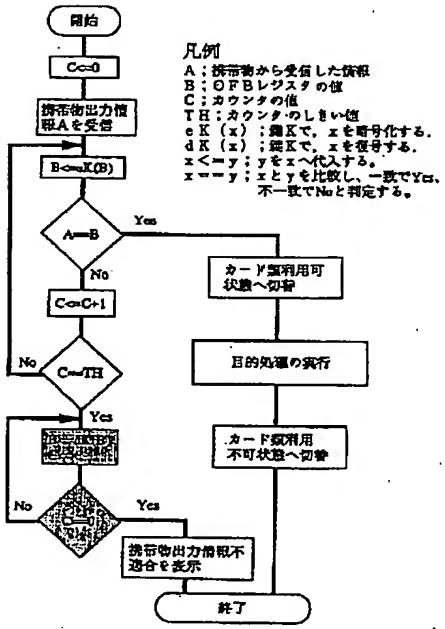
【図7】


開始
C<=0
携帯物出力情報Aを受信
B<=eK(B)
A==B
Yes
No
C<=C+1
C==TH
カード類利用可状態へ切替
カード類利用不可状態へ切替
携帯物出力情報不適合を表示
終了
凡例
A：携帯物から受信した情報
B：ＯＦＢレジスタの値
C：カウンタの値
TH：カウンタのしきい値
eK（x）：鍵Kで、xを暗号化する。
x<=y：yをxへ代入する。
x==y：xとyを比較し、一致でYes、不一致でNoと判定する。

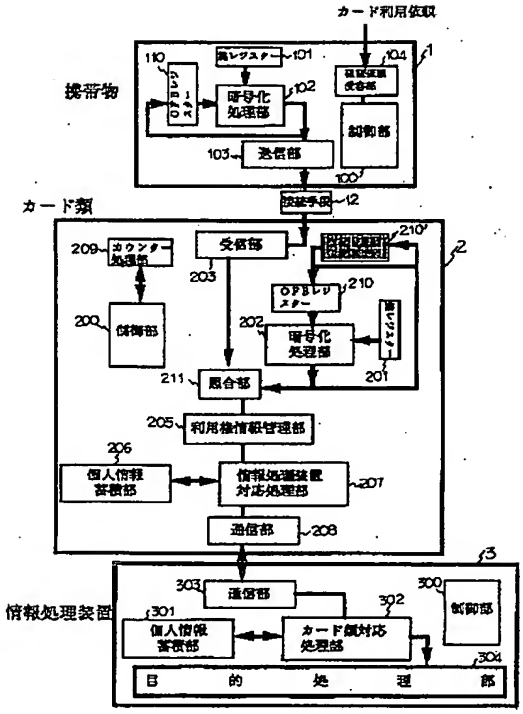
【図8】


カード利用依頼
携帯物
カード類
情報処理装置
暗号化処理部
送信部
制御部
受信部
照合部
利用者情報管理部
個人情報蓄積部
情報処理装置対応処理部
通信部
カード類対応処理部
目的処理部
携帯物対応設定

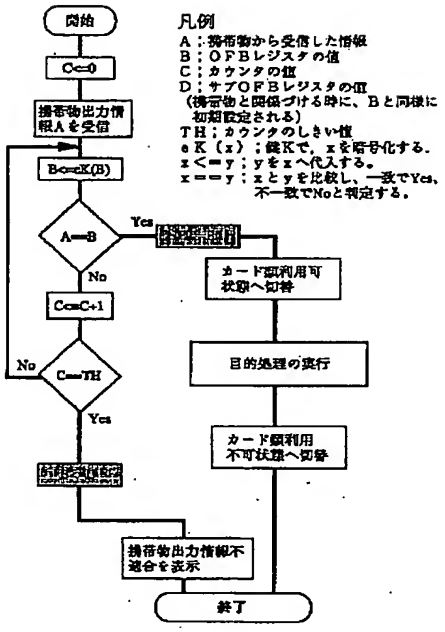
【図9】


開始
C<=0
携帯物出力情報Aを受信
B<=eK(B)
A==B
Yes
No
C<=C+1
C==TH
カード類利用可状態へ切替
目的処理の実行
カード類利用不可状態へ切替
携帯物出力情報不適合を表示
終了
凡例
A：携帯物から受信した情報
B：ＯＦＢレジスタの値
C：カウンタの値
TH：カウンタのしきい値
eK（x）：鍵Kで、xを暗号化する。
dK（x）：鍵Kで、xを復号する。
x<=y：yをxへ代入する。
x==y：xとyを比較し、一致でYes、不一致でNoと判定する。

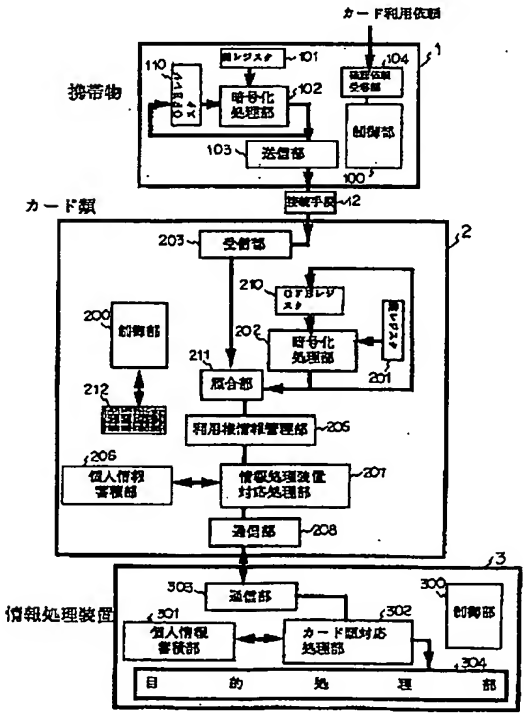
【図１０】



【図１１】



【図１２】

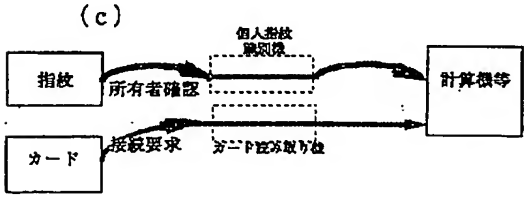


【図１４】

（a）

（b）

（c）



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	FI	技術表示箇所
Ｇ０６Ｋ　17/00		Ｓ　8623－5Ｌ		
Ｇ０７Ｆ　7/12				
Ｇ０９Ｃ　1/00		7922－5Ｌ		